

Contoso Legal LLP



PREPARED BY
Harbour IT

DATE
12 Oct 2026

DATA COLLECTED
12 Oct 2026, 17:16 UTC

MICROSOFT 365 TENANT
contoso.onmicrosoft.com

Everything collected about breakglass@contoso.example.

Needs attention

3

Worst: critical

Sign-in

Allowed

Last sign-in 12 days ago

MFA

No MFA

Admin roles

1

Global Administrator

Licences

None

Devices

None

Needs attention 3 3 to review

Flag	What	Area
Critical	No MFA: Not set up and not required: the password alone gets in. This account holds an admin role.	MFA and sign-in protection
Medium	Excluded from CA001 — Admins: Require phishing-resistant MFA, CA002 — All users: Require MFA, CA003 — Block legacy authentication, CA004 — All users: Require compliant or hybrid-joined device, CA005 — Block sign-ins from disallowed countries, CA006 — Require MFA for Azure management, CA007 — Admins: No persistent browser, 8h sign-in frequency, CA008 — All users: 8h sign-in frequency, CA009 — Require MFA for device registration, CA010 — Insider risk: Step-up MFA, CA011 — High sign-in risk: Block.	MFA and sign-in protection
Medium	Signed in 2 times with only a password in the last 7 days.	Recent sign-ins

Account 7

Detail	Value
Name	Emergency access
Sign-in name	breakglass@contoso.example
Account type	Member
Sign-in	Allowed
Source	Cloud-only
Created	4 Mar 2024 (952 days ago)
Password expires	Follows the organisation's policy

Licences 1

Note
Holds no licences.

Microsoft 365 use 1

Note
Not in Microsoft's usage reports for the last 30 days.

MFA and sign-in protection 10

Detail	Value
MFA set up	No
Methods	None

Detail	Value
Phishing-resistant method	No
Strongest method	None
Can sign in without a password	No
Can reset their own password	No
MFA required by	Nothing
Excluded from	CA001 — Admins: Require phishing-resistant MFA, CA002 — All users: Require MFA, CA003 — Block legacy authentication, CA004 — All users: Require compliant or hybrid-joined device, CA005 — Block sign-ins from disallowed countries, CA006 — Require MFA for Azure management, CA007 — Admins: No persistent browser, 8h sign-in frequency, CA008 — All users: 8h sign-in frequency, CA009 — Require MFA for device registration, CA010 — Insider risk: Step-up MFA, CA011 — High sign-in risk: Block
Conditional Access policies that apply	None
Legacy sign-in blocked	No

Admin roles 1

Role	How assigned	Scope	Privileged
Global Administrator	Active	Whole directory	Yes

Administrative units 1

Note
In no administrative unit, and administers none.

Teams and groups 1

Note

Not an owner or member of any team or group Office Sentry reads.

Mailbox 1

Note

No mailbox, and no access to anyone else's.

Devices 1

Note

No devices enrolled in Intune for this person.

OneDrive 1

Note

No OneDrive found for this account.

Apps this person allowed 1

Note

Hasn't consented to any app on their own behalf.

Recent sign-ins 6

Detail	Value
Successful	11 (9 with MFA, 2 with only a password)
Failed	None
MFA and other prompts	1
Countries	GB
Apps	Office 365 Exchange Online, Office 365 SharePoint Online, Microsoft Office, Microsoft Teams
Devices	Windows10

Where this account signed in 1

Country	Successful	Failed	Cities	IP addresses	Last success (UTC)
GB	11	0	London	203.0.113.26	9 Oct 2026, 17:01

Sign-in history 3

Detail	Value
History from	14 Jun 2026
Last sign-in	9 Oct 2026 (3 days ago)
Countries	GB, IE, US

Sign-ins by month 5

Flag	Month	Days	Successful	Failed	With MFA	Password only	Countries
● Low	Oct 2026	7	14	0	12	2	GB
● Low	Sep 2026	17	40	4	35	5	GB
● Low	Aug 2026	19	39	4	36	3	GB
● Low	Jul 2026	19	37	2	31	6	GB, US
● Low	Jun 2026	12	25	1	23	2	GB, IE

Sign-ins and admin changes 5

Detail	Value
Last interactive sign-in	30 Sep 2026 (12 days ago)
Last background sign-in	None recorded
Last successful sign-in	None recorded
Legacy sign-ins (30 days)	None
Admin changes (last 120 days)	None by or to this account

Timeline 1 1 to review

Flag	When	Area	What happened
● Medium	On or before 7 Sep 2026	Admin roles	Global Administrator role first seen

Open findings 5 5 to review

Flag	Check	Detail	First seen
Critical	Every admin has MFA registered	Global Administrator with no MFA method registered	7 Sep 2026
High	Every active user has MFA registered	No MFA method registered	7 Sep 2026
High	Every admin is covered by an MFA policy	Global Administrator: excluded from CA001 — Admins: Require phishing-resistant MFA, CA002 — All users: Require MFA, CA003 — Block legacy authentication, CA004 — All users: Require compliant or hybrid-joined device, CA005 — Block sign-ins from disallowed countries, CA006 — Require MFA for Azure management, CA007 — Admins: No persistent browser, 8h sign-in frequency, CA008 — All users: 8h sign-in frequency, CA009 — Require MFA for device registration, CA010 — Insider risk: Step-up MFA, CA011 — High sign-in risk: Block	7 Sep 2026
Medium	Admins use phishing-resistant sign-in methods	Global Administrator; signs in with no MFA method at all	7 Sep 2026
Medium	MFA is enforced for all users	Excluded from "CA002 — All users: Require MFA"	7 Sep 2026

History 0

No changes recorded yet.